

Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

A. Brooke Murphy (*pro hac vice* forthcoming)
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
abm@murphylegalfirm.com

Counsel for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

PROSPERO RODRIGUEZ and MARIA
RODRIGUEZ, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

NORTHWELL HEALTH, INC. and PERRY
JOHNSON & ASSOCIATES, INC.,

Defendants.

Case No. 2:23-cv-1874

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Prospero Rodriguez and Maria Rodriguez (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this Class Action Complaint, against defendants Northwell Health, Inc. (“Northwell”) and Perry Johnson & Associates (“PJA”) (collectively, “Defendants”) to obtain damages, restitution, and injunctive relief from Defendants. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach (“Data Breach”) resulting from Defendants’ failure to implement reasonable and industry standard data security practices to secure Plaintiffs’ and potentially millions other individuals’ personally identifying information (“PII”) and protected health information (“PHI”, and collectively with PII, “Private Information”), including names, Social Security numbers, dates of birth, addresses, medical record numbers, medical information, diagnosis information, provider information, and dates and times of service.

2. Northwell is the largest health system in New York.

3. PJA is a third-party vendor of health information technology solutions used by Northwell.

4. Plaintiffs and the Class Members (as further defined below) have had their Private Information exposed as a result of Defendants’ inadequately secured computer network. Defendants betrayed their obligations to Plaintiffs and the other Class Members by failing to properly safeguard and protect their PII and PHI and thereby enabling cybercriminals to steal such valuable and sensitive information.

5. Between approximately March 27, 2023 and May 2, 2023, an unauthorized third infiltrated PJA’s inadequately secured network, gained access to PJA’s computer system, and obtained files containing the Private Information of Northwell’s current and former patients (the “Data Breach”).

6. Private Information compromised in the Data Breach was downloaded by cyber-criminals and remains in the hands of those cyber-criminals who targeted the Private Information for its value to identity thieves.

1 7. As a result of the Data Breach, Plaintiffs and approximately 3.9 million Class
2 Members,¹ suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii)
3 theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time
4 and opportunity costs associated with attempting to mitigate the actual consequences of the Data
5 Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to
6 mitigate the actual consequences of the Data Breach; (vii) an increase in spam calls, texts, and/or
7 emails; and (viii) the continued and certainly increased risk to their Private Information, which: (a)
8 remains unencrypted and available for unauthorized third parties to access and abuse; and (b)
9 remains backed up in Defendants' possession and is subject to further unauthorized disclosures so
10 long as Defendants fail to undertake appropriate and adequate measures to protect the Private
11 Information.
12

13 8. The Data Breach was a direct result of Defendants' failure to implement adequate and
14 reasonable cyber-security procedures and protocols necessary to protect their patients' and their
15 clients' patients' Private Information from a foreseeable and preventable cyber-attack.
16

17 9. Defendants maintained the Private Information in a reckless manner. In particular,
18 the Private Information was maintained on Defendants' computer network and/or software platform
19 in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the
20 cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private
21 Information was a known risk to Defendants, and thus, Defendants were on notice that failing to
22 take steps necessary to secure the Private Information from those risks left that property in a
23 dangerous condition.
24

25
26
27
28 ¹ See <https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach>.

1 10. Defendants disregarded the rights of Plaintiffs and Class Members by, inter alia,
2 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures
3 to ensure their data systems were protected against unauthorized intrusions; failing to disclose that
4 they did not have adequately robust computer systems and security practices to safeguard Class
5 Members' Private Information; failing to take standard and reasonably available steps to prevent the
6 Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the
7 Data Breach.
8

9 11. Plaintiffs' and Class Members' identities are now at risk because of Defendants'
10 negligent conduct because the Private Information that Defendants collected and maintained is now
11 in the hands of data thieves.
12

13 12. Armed with the Private Information accessed in the Data Breach, data thieves have
14 already engaged in identity theft and fraud and can in the future commit a variety of crimes including,
15 e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members'
16 names, using Class Members' information to obtain government benefits, filing fraudulent tax
17 returns using Class Members' information, obtaining driver's licenses in Class Members' names but
18 with another person's photograph, and giving false information to police during an arrest.
19

20 13. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a
21 heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now
22 and in the future closely monitor their financial accounts to guard against identity theft.

23 14. Plaintiffs and Class Members may also incur out of pocket costs, e.g., for purchasing
24 credit monitoring services, credit freezes, credit reports, or other protective measures to deter and
25 detect identity theft.

26 15. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to
27 address Defendants' inadequate safeguarding of Class Members' Private Information that it collected
28 and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class

1 Members that their information had been subject to the unauthorized access by an unknown third
2 party and precisely what specific type of information was accessed.

3 16. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of
4 themselves and all similarly situated individuals whose Private Information was accessed during the
5 Data Breach.

6 17. Plaintiff seek remedies including, but not limited to, compensatory damages and
7 injunctive relief including improvements to Defendants' data security systems, future annual audits,
8 and adequate credit monitoring services funded by Defendants.

9 **II. PARTIES**

10 18. Plaintiff Prospero Rodriguez, and at all times mentioned herein was, an individual
11 citizen of the State of New York.

12 19. Plaintiff Maria Rodriguez is, and at all times mentioned herein was, an individual
13 citizen of the State of New York.

14 20. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its
15 principal place of business at 2000 Marcus Ave., New Hyde Park, NY 11042.

16 21. Defendant Perry Johnson & Associates is a Nevada corporation with its principal
17 place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. It may be served through its
18 registered agent CT Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

19 **III. JURISDICTION AND VENUE**

20 22. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. §
21 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a
22 citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy
23 exceeds \$5,000,000, exclusive of interest and costs.

24 23. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc.
25 because it is a corporation incorporated under the laws of Nevada, has its principal place of business
26

1 in Nevada, and does significant business in Nevada.

2 24. This Court has personal jurisdiction over Northwell because transacts business within
3 this state and makes or performs contracts within this state.

4 25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJA has
5 its principal place of business in Nevada, and a substantial part of the events giving rise to Plaintiffs'
6 claims arose in this District.

8 **IV. FACTUAL ALLEGATIONS**

9 **A. *Defendants' Business and The Data Breach***

10 26. Northwell is the largest health system in New York. It employs more than 85,000
11 people at over 900 locations.²

12 27. In the regular course of its business, Northwell collects and maintains the PII/PHI of
13 its current and former patients. Northwell required Plaintiff and Class members to provide their
14 Private Information as a condition of receiving healthcare services from Northwell.

15 28. Defendant PJA is a medical transcription service vendor. To perform these services,
16 PJA receives and stores PII and PHI from medical providers, including Northwell. Upon information
17 and belief, Defendant PJA developed and maintained the computer network that was the subject of
18 the Data Breach.

19 29. In the course of their relationship, patients of Northwell, including Plaintiffs and
20 Class Members, provided Defendants, directly or indirectly, with at least the following information:
21 names, dates of birth, addresses, emails, Social Security numbers, driver's licenses, health insurance
22 information, and medical treatment and/or diagnosis information.
23
24

25
26
27
28 ² <https://www.northwell.edu/about-northwell>.

1 30. Between approximately March 27, 2023 and May 2, 2023, an unauthorized third
2 infiltrated PJA's inadequately secured network, gained access to PJA's computer system, and
3 "acquired copies of certain files" containing the Private Information of Northwell's current and
4 former patients.³

5
6 31. According to PJA, the PII and PHI affected in the Data Breach includes, names, dates
7 of birth, Social Security numbers, addresses, medical record numbers, hospital account numbers,
8 admission diagnosis, insurance information, and clinical information (such as laboratory and
9 diagnosis testing results, medications, names of treatment facilities, and healthcare provider
10 names).⁴

11 32. The files containing Plaintiffs' and Class Members' Private Information, were
12 targeted and stolen from Defendants.

13
14 33. Because of this targeted cyberattack, data thieves were able to gain access to and
15 obtain data from Defendants that included the Private Information of Plaintiffs and Class Members.

16 34. As evidenced by the Data Breach's occurrence, the Private Information contained in
17 Defendants' network was not encrypted. Had the information been properly encrypted, the data
18 thieves would have exfiltrated only unintelligible data.

19 35. Defendants had obligations created by the FTC Act, HIPAA, contract, state and
20 federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private
21 Information confidential and to protect it from unauthorized access and disclosure.

22
23 36. Moreover, Northwell's Notice of Privacy Practices states, "You have a right to be
24 notified in the event of a breach of the privacy of your unsecured protected health information by
25
26
27

28 ³ <https://www.pjats.com/downloads/Notice.pdf>.

⁴ *Id.*

Northwell Health or its business associates.”⁵ It promises patients that they “will be notified as soon as reasonably possible, but no later than 60 days following our discovery of the breach.”⁶ PJA informed Northwell of the Data Breach on July 21, 2023,⁷ but Northwell failed to notify its patients until early November, 2023, over three months later after its discovery of the breach.

B. Data Breaches Are Preventable

37. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

38. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

39. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁸

40. To prevent and detect cyber-attacks and/or ransomware attacks Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF),

⁵ <https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf>.

⁶ *Id.*

⁷ <https://www.pjats.com/downloads/Notice.pdf>.

⁸ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁹

⁹ *Id.* at 3-4.

1 41. To prevent and detect cyber-attacks or ransomware attacks Defendants could and
2 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
3 the following measures:

4 **Secure internet-facing assets**

- 5 - Apply latest security updates
6 - Use threat and vulnerability management
7 - Perform regular audit; remove privileged credentials;

8 **Thoroughly investigate and remediate alerts**

- 9 - Prioritize and treat commodity malware infections as potential full compromise;

10 **Include IT Pros in security discussions**

- 11 - Ensure collaboration among [security operations], [security admins], and
12 [information technology] admins to configure servers and other endpoints securely;

13 **Build credential hygiene**

- 14 - Use [multifactor authentication] or [network level authentication] and use strong,
15 randomized, just-in-time local admin passwords;

16 **Apply principle of least-privilege**

- 17 - Monitor for adversarial activities
18 - Hunt for brute force attempts
19 - Monitor for cleanup of Event Logs
20 - Analyze logon events;

21 **Harden infrastructure**

- 22 - Use Windows Defender Firewall
23 - Enable tamper protection
24 - Enable cloud-delivered protection
25
26
27
28

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].¹⁰

42. Given that Defendants were storing the sensitive Private Information of NORTHWELL's current and former patients as well as their clients' current and former patients, Defendants could and should have implemented all of the above measures to prevent and detect cyberattacks.

43. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the unencrypted Private Information of approximately 3.9 million patients,¹¹ including that of Plaintiffs and Class Members.

C. *Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' Private Information*

44. Defendants acquire, collect, and store a massive amount of Private Information in the regular course of their business.

45. As a condition of obtaining medical services or products at NORTHWELL and/or NORTHWELL's clients, NORTHWELL requires that patients, former patients, and other personnel—including Plaintiffs and Class Members—entrust it with highly sensitive personal information.

46. Companies providing services to the healthcare industry, such as PJA, was obligated to reasonably protect the highly sensitive Private Information it assisted in storing and maintaining.

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

¹¹ See <https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach>.

1 47. By obtaining, collecting, and using Plaintiffs' and Class Members' Private
2 Information, Defendants assumed legal and equitable duties and knew or should have known that it
3 was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

4 48. Plaintiffs and Class Members have taken reasonable steps to maintain the
5 confidentiality of their Private Information and would not have entrusted it to Defendants absent an
6 implied promise to safeguard that information.

7 49. Plaintiffs and the Class Members relied on Defendants to keep their Private
8 Information confidential and securely maintained, to use this information for business purposes only,
9 and to make only authorized disclosures of this information.

10
11 **D. *Defendants Knew or Should Have Known of the Risk Because Healthcare***
12 ***Entities in Possession Of Private information Are Particularly Susceptable***
13 ***To Cyber Attacks***

14 50. Defendants' data security obligations were particularly important given the
15 substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect
16 and store Private Information, like Defendants, preceding the date of the breach.

17 51. Data breaches, including those perpetrated against healthcare entities, and companies
18 providing services to healthcare entities, that store Private Information in their systems, have become
19 widespread.

20 52. In 2021, a record 1,862 data breaches occurred, resulting in approximately
21 293,927,708 sensitive records being exposed, a 68% increase from 2020.¹²

22 53. In light of recent high profile cybersecurity incidents at other healthcare partner and
23 provider companies, including American Medical Collection Agency (25 million patients, March
24 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic
25
26

27
28 ¹² See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at
<https://notified.idtheftcenter.org/s/>), at 6.

Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

54. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹³

55. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants’ data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

56. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

¹³ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consume_rprotection (last accessed Oct. 17, 2022).

1 57. The injuries to Plaintiffs and Class Members were directly and proximately caused
2 by Defendants' failure to implement or maintain adequate data security measures for the Private
3 Information of Plaintiffs and Class Members.

4 58. The ramifications of Defendants' failure to keep secure the Private Information of
5 Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—
6 particularly Social Security numbers and PHI—fraudulent use of that information and damage to
7 victims may continue for years.

9 **E. Value of Private Information**

10 59. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed
11 or attempted using the identifying information of another person without authority."¹⁴ The FTC
12 describes "identifying information" as "any name or number that may be used, alone or in
13 conjunction with any other information, to identify a specific person," including, among other things,
14 "[n]ame, Social Security number, date of birth, official State or government issued driver's license
15 or identification number, alien registration number, government passport number, employer or
16 taxpayer identification number."¹⁵

17 60. The PII of individuals remains of high value to criminals, as evidenced by the prices
18 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
19 credentials.¹⁶

20 61. For example, Personal Information can be sold at a price ranging from \$40 to \$200.¹⁷

21
22
23
24
25 ¹⁴ 17 C.F.R. § 248.201 (2013).

26 ¹⁵ *Id.*

27 ¹⁶ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
28 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

¹⁷ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6,
2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

1 Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁸

2 62. For example, Social Security numbers are among the worst kind of Private
3 Information to have stolen because they may be put to a variety of fraudulent uses and are difficult
4 for an individual to change. The Social Security Administration stresses that the loss of an
5 individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead
6 to identity theft and extensive financial fraud:
7

8 A dishonest person who has your Social Security number can use it to get other
9 personal information about you. Identity thieves can use your number and your good
10 credit to apply for more credit in your name. Then, they use the credit cards and don't
11 pay the bills, it damages your credit. You may not find out that someone is using your
12 number until you're turned down for credit, or you begin to get calls from unknown
13 creditors demanding payment for items you never bought. Someone illegally using
14 your Social Security number and assuming your identity can cause a lot of
15 problems.¹⁹

16 63. What's more, it is no easy task to change or cancel a stolen Social Security number.
17 An individual cannot obtain a new Social Security number without significant paperwork and
18 evidence of actual misuse. In other words, preventive action to defend against the possibility of
19 misuse of a Social Security number is not permitted; an individual must show evidence of actual,
20 ongoing fraud activity to obtain a new number.

21 64. Even then, a new Social Security number may not be effective. According to Julie
22 Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the
23 new number very quickly to the old number, so all of that old bad information is quickly inherited
24 into the new Social Security number."²⁰

25 ¹⁸ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

26 ¹⁹ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
27 <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

28 ²⁰ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR
(Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft>.

65. Theft of PHI is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²¹

66. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.²²

67. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number, PHI, and name.

68. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²³

69. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

70. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

²¹ *What To Know About Medical Identity Theft*, Federal Trade Commission, (May 2021), available at <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft>.

²² Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content>.

²³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

1 between when Private Information is stolen and when it is used. According to the U.S. Government
 2 Accountability Office (“GAO”), which conducted a study regarding data breaches:

3 [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a
 4 year or more before being used to commit identity theft. Further, once stolen data have been
 5 sold or posted on the Web, fraudulent use of that information may continue for years. As a
 6 result, studies that attempt to measure the harm resulting from data breaches cannot
 necessarily rule out all future harm.²⁴

7 71. Plaintiffs and Class Members now face years of constant surveillance of their
 8 financial and personal records, monitoring, and loss of rights. The Class is incurring and will
 9 continue to incur such damages in addition to any fraudulent use of their Private Information.

10 **F. Defendants Fail to Comply with FTC Guidelines**

11 72. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
 12 businesses which highlight the importance of implementing reasonable data security practices.
 13 According to the FTC, the need for data security should be factored into all business decision-
 14 making.
 15

16 73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide
 17 for Business, which established cyber-security guidelines for businesses. These guidelines note that
 18 businesses should protect the personal patient information that they keep; properly dispose of
 19 personal information that is no longer needed; encrypt information stored on computer networks;
 20 understand their network’s vulnerabilities; and implement policies to correct any security
 21 problems.²⁵
 22

23 74. The guidelines also recommend that businesses use an intrusion detection system to
 24 expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is
 25

26
 27 ²⁴ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
<https://www.gao.gov/assets/gao-07-737.pdf>.

28 ²⁵ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).
 Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

1 attempting to hack the system; watch for large amounts of data being transmitted from the system;
2 and have a response plan ready in the event of a breach.²⁶

3 75. The FTC further recommends that companies not maintain Private Information
4 longer than is needed for authorization of a transaction; limit access to sensitive data; require
5 complex passwords to be used on networks; use industry-tested methods for security; monitor for
6 suspicious activity on the network; and verify that third-party service providers have implemented
7 reasonable security measures.

9 76. The FTC has brought enforcement actions against businesses for failing to adequately
10 and reasonably protect patient data, treating the failure to employ reasonable and appropriate
11 measures to protect against unauthorized access to confidential consumer data as an unfair act or
12 practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.
13 Orders resulting from these actions further clarify the measures businesses must take to meet their
14 data security obligations.

16 77. These FTC enforcement actions include actions against healthcare entities, like
17 Defendants. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016
18 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data
19 security practices were unreasonable and constitute an unfair act or practice in violation of Section
20 5 of the FTC Act.”).

22 78. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting
23 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by
24 businesses, such as Defendants, of failing to use reasonable measures to protect Private Information.
25 The FTC publications and orders described above also form part of the basis of Defendants’ duty in
26 this regard.

28 ²⁶ *Id.*

1 79. Defendants failed to properly implement basic data security practices.

2 80. Defendants' failure to employ reasonable and appropriate measures to protect against
3 unauthorized access to patients' Private Information or to comply with applicable industry standards
4 constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.
5

6 81. Upon information and belief, Defendants were at all times fully aware of their
7 obligation to protect the Private Information of their patients' and their clients' patients. Defendants
8 were also aware of the significant repercussions that would result from their failure to do so.
9 Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of
10 Private Information it obtained and stored and the foreseeable consequences of the immense
11 damages that would result to Plaintiffs and the Class.
12

13 **G. *Defendants Fail to Comply with HIPAA Guidelines***

14 82. Defendants were covered business associates under HIPAA (45 C.F.R. § 160.103)
15 and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and
16 Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"),
17 and Security Rule ("Security Standards for the Protection of Electronic Protected Health
18 Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.
19

20 83. Defendants are subject to the rules and regulations for safeguarding electronic forms
21 of medical information pursuant to the Health Information Technology Act ("HITECH").²⁷ See 42
22 U.S.C. §17921, 45 C.F.R. § 160.103.

23 84. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health*
24 *Information* establishes national standards for the protection of health information.
25
26
27

28 ²⁷ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

1 85. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic*
 2 *Protected Health Information* establishes a national set of security standards for protecting health
 3 information that is kept or transferred in electronic form.

4 86. HIPAA requires "compl[iance] with the applicable standards, implementation
 5 specifications, and requirements" of HIPAA "with respect to electronic protected health
 6 information." 45 C.F.R. § 164.302.

7 87. "Electronic protected health information" is "individually identifiable health
 8 information ... that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R.
 9 § 160.103.

10 88. HIPAA's Security Rule requires Defendants to do the following:

- 11 a. Ensure the confidentiality, integrity, and availability of all electronic protected health
- 12 information the covered entity or business associate creates, receives, maintains, or
- 13 transmits;
- 14 b. Protect against any reasonably anticipated threats or hazards to the security or
- 15 integrity of such information;
- 16 c. Protect against any reasonably anticipated uses or disclosures of such information
- 17 that are not permitted; and
- 18 d. Ensure compliance by their workforce.

19 89. HIPAA also requires Defendants to "review and modify the security measures
 20 implemented ... as needed to continue provision of reasonable and appropriate protection of
 21 electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendants are
 22 required under HIPAA to "[i]mplement technical policies and procedures for electronic information
 23 systems that maintain electronic protected health information to allow access only to those persons
 24 or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).
 25
 26
 27
 28

1 90. HIPAA and HITECH also obligated Defendants to implement policies and
 2 procedures to prevent, detect, contain, and correct security violations, and to protect against uses or
 3 disclosures of electronic protected health information that are reasonably anticipated but not
 4 permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C.
 5 §17902.

6
 7 91. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires
 8 Defendants to provide notice of the Data Breach to each affected individual “without unreasonable
 9 delay and in no case later than 60 days following discovery of the breach.”²⁸

10 92. HIPAA requires a covered entity to have and apply appropriate sanctions against
 11 members of its workforce who fail to comply with the privacy policies and procedures of the covered
 12 entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

13 93. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful
 14 effect that is known to the covered entity of a use or disclosure of protected health information in
 15 violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the
 16 covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

17 94. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of
 18 Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the
 19 HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed
 20 guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost
 21 effective and appropriate administrative, physical, and technical safeguards to protect the
 22 confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements
 23 of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance
 24
 25
 26

27
 28 ²⁸ Breach Notification Rule, U.S. Dep’t of Health & Human Services,
<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added).

Material.²⁹ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.³⁰

H. *Defendants fail to Comply with Industry Standards*

95. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

96. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

97. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

²⁹ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html>.

³⁰ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html>

1 98. Defendants failed to meet the minimum standards of any of the following
2 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-
3 1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1,
4 PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet
5 Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable
6 cybersecurity readiness.

7
8 99. These foregoing frameworks are existing and applicable industry standards in the
9 healthcare industry, and upon information and belief, Defendants failed to comply with at least one—
10 —or all—of these accepted standards, thereby opening the door to the threat actor and causing the
11 Data Breach.

12 **I. Common Injuries & Damages**

13
14 100. As a result of Defendants' ineffective and inadequate data security practices, the Data
15 Breach, and the foreseeable consequences of Private Information ending up in the possession of
16 criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is
17 imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages,
18 including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk
19 and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the
20 materialized risk and imminent threat of identity theft risk; (d) loss of time due to increased spam
21 and targeted marketing emails; (e) the loss of benefit of the bargain (price premium damages); (f)
22 diminution of value of their Private Information; and (g) the continued risk to their Private
23 Information, which remains in the possession of Defendants, and which is subject to further
24 breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect
25 Plaintiffs' and Class Members' Private Information.
26

27 **J. The Data Breach Increases Victims' Risk of Identity Theft**
28

1 101. Unencrypted Private Information may also fall into the hands of companies that will
2 use the detailed Private Information for targeted marketing without the approval of Plaintiffs and
3 Class Members. Simply, unauthorized individuals can easily access the Private Information of
4 Plaintiffs and Class Members.

5 102. The link between a data breach and the risk of identity theft is simple and well
6 established. Criminals acquire and steal Private Information to monetize the information. Criminals
7 monetize the data by selling the stolen information on the black market to other criminals who then
8 utilize the information to commit a variety of identity theft related crimes discussed below.

9 103. Plaintiffs' and Class Members' Private Information is of great value to hackers and
10 cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used
11 in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off
12 their misfortune.

13 104. Because a person's identity is akin to a puzzle, the more accurate pieces of data an
14 identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or
15 otherwise harass or track the victim. For example, armed with just a name and date of birth, a data
16 thief can utilize a hacking technique referred to as "social engineering" to obtain even more
17 information about a victim's identity, such as a person's login credentials or Social Security number.
18 Social engineering is a form of hacking whereby a data thief uses previously acquired information
19 to manipulate individuals into disclosing additional confidential or personal information through
20 means such as spam phone calls and text messages or phishing emails.

21 105. In fact, as technology advances, computer programs may scan the Internet with a
22 wider scope to create a mosaic of information that may be used to link compromised information to
23 an individual in ways that were not previously possible. This is known as the "mosaic effect."

106. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.³¹

107. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

108. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

³¹ “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/>.

109. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

110. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

K. *Loss of Time to Mitigate the Risk of Identity Theft and Fraud*

111. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

112. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendants’ Notice Letter instructs,³² “remain vigilant” and monitor their financial accounts for many years to mitigate the risk of identity theft.

113. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, contacting financial institutions to ensure their financial accounts are secured, exploring credit monitoring and identity theft insurance options, seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach, researching

³² Notice Letter.

1 how best to ensure that they are protected from identity theft, reviewing account statements and other
2 information for any indication of fraudulent activity, which may take years to detect.

3 114. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability
4 Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that
5 victims of identity theft will face "substantial costs and time to repair the damage to their good name
6 and credit record."³³

7
8 115. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends
9 that data breach victims take several steps to protect their personal and financial information after a
10 data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an
11 extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit
12 reports, contacting companies to remove fraudulent charges from their accounts, placing a credit
13 freeze on their credit, and correcting their credit reports.³⁴

14
15 **L. *Diminution of Value of PII and PHI***

16 116. PII and PHI are valuable property rights.³⁵ Their value is axiomatic, considering the
17 value of Big Data in corporate America and the consequences of cyber thefts include heavy prison
18 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information
19 has considerable market value.
20
21
22
23
24

25 ³³ See United States Government Accountability Office, GAO-07-737, Personal Information: Data
26 Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full
27 Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁴ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps>.

³⁵ See "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> ("GAO Report").

1 117. Sensitive PII can sell for as much as \$363 per record according to the Infosec
2 Institute.³⁶

3 118. An active and robust legitimate marketplace for PII also exists. In 2019, the data
4 brokering industry was worth roughly \$200 billion.³⁷ In fact, the data marketplace is so sophisticated
5 that consumers can actually sell their non-public information directly to a data broker who in turn
6 aggregates the information and provides it to marketers or app developers.^{38,39} Consumers who agree
7 to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁰

8 119. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information,
9 which has an inherent market value in both legitimate and dark markets, has been damaged and
10 diminished by its compromise and unauthorized release. However, this transfer of value occurred
11 without any consideration paid to Plaintiffs or Class Members for their property, resulting in an
12 economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data
13 has been lost, thereby causing additional loss of value.

14 120. At all relevant times, Defendants knew, or reasonably should have known, of the
15 importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the
16 foreseeable consequences that would occur if Defendants' data security system was breached,
17 including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members
18 as a result of a breach.
19
20
21
22

23
24 ³⁶ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable
25 Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech.
26 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable
value that is rapidly reaching a level comparable to the value of traditional financial assets.")
(citations omitted).

27 ³⁷ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
<https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

28 ³⁸ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

³⁹ <https://datacoup.com/>

⁴⁰ <https://digi.me/what-is-digime/>

121. The fraudulent activity resulting from the Data Breach may not come to light for years.

122. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information .

123. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to potentially over three hundred thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

124. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

M. *Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary*

125. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, the volume of Private Information impacted in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

126. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected

1 fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return
2 is rejected.

3 127. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and
4 identity theft for many years into the future.

5 128. The retail cost of credit monitoring and identity theft monitoring can cost around
6 \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class
7 Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future
8 cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for
9 Defendants' failure to safeguard their Private Information .
10

11 **N. *Loss of Benefit of the Bargain***

12 129. Furthermore, Defendants' poor data security deprived Plaintiffs and Class Members
13 of the benefit of their bargain. When agreeing to pay Defendants and/or Defendants' clients for
14 medical services, Plaintiffs and other reasonable consumers understood and expected that they were,
15 in part, paying for the service that provided the necessary data security to protect their Private
16 Information, when in fact, Defendants did not provide the expected data security. Accordingly,
17 Plaintiffs and Class Members received services that were of a lesser value than what they reasonably
18 expected to receive under the bargains they struck with Defendants and/or Defendants' clients.
19

20 **O. *Plaintiffs' Experiences***

21 130. Plaintiffs are former patients of Northwell.

22 131. In order to obtain medical services through Northwell, they were required to provide
23 their Private Information, indirectly or directly, to Northwell.
24

25 132. Upon information and belief, at the time of the Data Breach, Northwell retained
26 Plaintiffs' Private Information in its system. Upon information and belief, Northwell then provided
27 Plaintiffs' Private Information to PJA.
28

1 133. Plaintiffs are very careful about sharing their sensitive Private Information. Plaintiffs
2 stores any documents containing their Private Information in a safe and secure location. Plaintiffs
3 have never knowingly transmitted unencrypted sensitive Private Information over the internet or any
4 other unsecured source. Plaintiffs would not have entrusted their Private Information to Defendants
5 had he known of Defendants' lax data security policies.

6 134. Plaintiffs both received breach notification letters, by U.S. mail, directly from PJA,
7 dated November 3, 2023. According to the notice letters, Plaintiffs' Private Information was
8 improperly accessed and obtained by unauthorized third parties during the Data Breach.

9 135. As a result of the Data Breach, and at the direction of PJA's notice letters, Plaintiffs
10 have made reasonable efforts to mitigate the impact of the Data Breach, including researching the
11 data breach, researching information about how best to protect their information, reviewing financial
12 account statements and other information, and taking other steps in an attempt to mitigate the current
13 and future harms caused by the Data Breach. Plaintiffs have spent significant time dealing with the
14 Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but
15 not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

16 136. Plaintiffs suffered actual injury from having their Private Information compromised
17 as a result of the Data Breach including, but not limited to: (i) lost or diminished value of his Private
18 Information; (ii) lost opportunity costs associated with attempting to mitigate the actual
19 consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy;
20 (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his Private
21 Information, which: (a) remains unencrypted and available for unauthorized third parties to access
22 and abuse; and (b) remains backed up in Defendants' possession and is subject to further
23 unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures
24 to protect the Private Information.
25
26
27
28

1 137. The Data Breach has caused Plaintiffs to suffer fear, anxiety, and stress, which has
2 been compounded by the fact that Defendants has still not fully informed them of key details about
3 the Data Breach's occurrence.

4 138. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and
5 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.
6

7 139. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be
8 at increased risk of identity theft and fraud for years to come.

9 140. Plaintiffs have a continuing interest in ensuring that their Private Information, which,
10 upon information and belief, remains backed up in Defendants' possession, is protected and
11 safeguarded from future breaches.

12 V. CLASS ACTION ALLEGATIONS

13
14 141. Plaintiffs bring this action individually and on behalf of all other persons similarly
15 situated, pursuant to Federal Rule of Civil Procedure 23.

16 142. Specifically, Plaintiffs propose the following Class (referred to herein as the "Class"
17 or "Class Members"), subject to amendment as appropriate:

18 All individuals who reside in the United States whose Private Information was exposed in
19 the Data Breach (the "Class").

20 143. Excluded from the Class are Defendants and their parents or subsidiaries, any entities
21 in which it has a controlling interest, as well as their officers, directors, affiliates, legal
22 representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom
23 this case is assigned as well as their judicial staff and immediate family members.

24 144. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class,
25 as well as add subclasses, before the Court determines whether certification is appropriate.
26

27 145. The proposed Classes meet the criteria for certification under Rule 23.
28

146. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of approximately 3.9 million patients whose data was compromised in the Data Breach.⁴¹ The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

147. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendants engaged in the conduct alleged herein;
- b. Whether Defendants' conduct violated the FTCA and/or HIPAA;
- c. When Defendants learned of the Data Breach;
- d. Whether Defendants' response to the Data Breach was adequate;
- e. Whether Defendants unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;
- f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;
- g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

⁴¹ See <https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach>.

- i. Whether Defendants owed a duty to Class Members to safeguard their Private Information;
- j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;
- k. Whether hackers obtained Class Members' Private Information via the Data Breach;
- l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;
- m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- n. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- o. What damages Plaintiffs and Class Members suffered as a result of Defendants' misconduct;
- p. Whether Defendants' conduct was negligent;
- q. Whether Defendants' conduct was *per se* negligent;
- r. Whether Defendants were unjustly enriched;
- s. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- t. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and
- u. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

1 148. Typicality. Plaintiffs' claims are typical of those of other Class Members because
2 Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data
3 Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all
4 Class Members were injured through the common misconduct of Defendants. Plaintiffs are
5 advancing the same claims and legal theories on behalf of themselves and all other Class Members,
6 and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class
7 Members arise from the same operative facts and are based on the same legal theories.
8

9 149. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests of
10 Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions,
11 including data privacy litigation of this kind.
12

13 150. Predominance. Defendants has engaged in a common course of conduct toward
14 Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the
15 same computer systems and unlawfully accessed and exfiltrated in the same way. The common
16 issues arising from Defendants' conduct affecting Class Members set out above predominate over
17 any individualized issues. Adjudication of these common issues in a single action has important and
18 desirable advantages of judicial economy.
19

20 151. Superiority. A Class action is superior to other available methods for the fair and
21 efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in
22 the management of this class action. Class treatment of common questions of law and fact is superior
23 to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members
24 would likely find that the cost of litigating their individual claims is prohibitively high and would
25 therefore have no effective remedy. The prosecution of separate actions by individual Class Members
26 would create a risk of inconsistent or varying adjudications with respect to individual Class
27 Members, which would establish incompatible standards of conduct for Defendants. In contrast,
28

conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

152. Defendants has also acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

153. Finally, all members of the proposed Class are readily ascertainable. Defendants has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

VI. CLAIMS FOR RELIEF

COUNT I

Negligence

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

154. Plaintiffs restate and reallege all of the allegations stated above as if fully set forth herein.

155. Defendants knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

156. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, they knew or should have known that they would be an attractive target for cyberattacks.

157. Defendants owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. Defendants' duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;
- b. To protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in their possession;
- d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;
- e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and
- f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

158. Defendants' duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Defendants' duty also arose because Defendants were bound by industry standards to protect their patients' and their clients' patients' confidential Private Information.

160. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

161. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within Defendants' possession.

1 162. Defendants, by their actions and/or omissions, breached their duty of care by failing
2 to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and
3 data security practices to safeguard the Private Information of Plaintiffs and Class Members.

4 163. Defendants, by their actions and/or omissions, breached their duty of care by failing
5 to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach
6 to the persons whose Private Information was compromised.

7 164. Defendants breached their duties, and thus was negligent, by failing to use reasonable
8 measures to protect Class Members' Private Information. The specific negligent acts and omissions
9 committed by Defendants include, but are not limited to, the following:

- 10
- 11 a. Failing to adopt, implement, and maintain adequate security measures to safeguard
 - 12 Class Members' Private Information;
 - 13 b. Failing to adequately monitor the security of their networks and systems;
 - 14 c. Failing to periodically ensure that their email system maintained reasonable data
 - 15 security safeguards;
 - 16 d. Allowing unauthorized access to Class Members' Private Information; and
 - 17 e. Failing to comply with the FTCA and/or HIPAA.
- 18

19 165. Defendants had a special relationship with Plaintiffs and Class Members. Plaintiffs'
20 and Class Members' willingness to entrust Defendants with their Private Information was predicated
21 on the understanding that Defendants would take adequate security precautions. Moreover, only
22 Defendants had the ability to protect their systems (and the Private Information that it stored on
23 them) from attack.

24 166. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs'
25 and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.
26
27
28

1 167. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members
2 regarding exactly what Private Information has been compromised, Plaintiffs and Class Members
3 have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

4 168. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiffs
5 and Class Members of identity theft, loss of control over their Private Information, and/or loss of
6 time and money to monitor their accounts for fraud.

7 169. As a result of Defendants' negligence in breach of their duties owed to Plaintiffs and
8 Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private
9 Information, which is still in the possession of third parties, will be used for fraudulent purposes.

10 170. Defendants also had independent duties under state laws that required it to reasonably
11 safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the
12 Data Breach.

13 171. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and
14 Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

15 172. The injury and harm that Plaintiffs and Class Members suffered was reasonably
16 foreseeable.

17 173. Plaintiffs and Class Members have suffered injury and are entitled to damages in an
18 amount to be proven at trial.

19 174. In addition to monetary relief, Plaintiffs and Class Members are also entitled to
20 injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and
21 monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit
22 monitoring and identity theft insurance to Plaintiffs and Class Members.

23 **COUNT II**
24 **Breach of Implied Contract**
25 **(On Behalf of Plaintiffs and the Class Against Northwell)**
26

1 175. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as
2 though fully set forth herein.

3 176. Plaintiffs and Class Members were required to provide Northwell with their Private
4 Information in order to receive medical care and treatment.

5 177. When Plaintiffs and Class Members provided their Private Information to Northwell
6 when seeking medical services, they entered into implied contracts in which Northwell agreed to
7 comply with its statutory and common law duties to protect their Private Information and to timely
8 notify them in the event of a Data Breach.

9 178. Plaintiffs would not have provided their PII to Northwell had they known that
10 Defendant would not safeguard their PII, as promised, or provide timely notice of the Data Breach.

11 179. Based on Northwell's representations (including those in its Privacy Policy), legal
12 obligations, and acceptance of Plaintiff's and the Class Members' Private Information, Defendant
13 had an implied duty to safeguard their Private Information through the use of reasonable industry
14 standards.

15 180. Indeed, Northwell's Privacy Policy makes clear that it understands that its patients'
16 Private Information is personal and must be protected by law. The Privacy Policy "explains how
17 [Northwell will] fulfill [its] commitment to respect the privacy and confidentiality of your protected
18 health information."⁴² The Privacy Policy further asserts: "We are required by law to make sure that
19 information the identifies you is kept private[.]"⁴³

20 181. Defendant's conduct and statements confirm that Defendant intended to bind itself to
21 protect the PII that Plaintiffs and the Nationwide Class entrusted to Defendant.

22
23
24
25
26
27 ⁴² <https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf>.

28 ⁴³ *Id.*

182. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

183. Defendant, however, breached the implied contracts by failing to safeguard Plaintiff's and Class Members' Private Information and failing to provide them with timely and accurate notice of the Data Breach. In particular, Defendant breached the implied contracts by (i) failing to use commercially reasonable physical, managerial, and technical safeguards to preserve the integrity and security of Plaintiffs' and the Class's Private Information, (ii) failing to encrypt the highly sensitive Private Information, including Social Security Numbers and PHI, (iii) failing to delete Private Information it no longer had a reasonable need to maintain, (iv) otherwise failing to safeguard and protect their PII, and (v) failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

184. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' Private Information.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs and the Class Against Northwell)

185. Plaintiffs incorporate by reference the foregoing paragraphs as if fully set forth herein.

186. At all relevant times hereto, Northwell owed, and owes, a fiduciary duty to Plaintiffs and the Class, including its duty to keep Plaintiffs and Class Members' Private Information reasonably secure.

187. The fiduciary duty is explicated under the procedures set forth in the Health Insurance Portability and Accountability Act Privacy Rule, including, without limitation the procedures and definitions of 45 C.F.R. §160.103 and 45 C.F.R. §164.530, which required Defendant to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient

1 information and to secure the health care information it maintains and to keep it free from
2 disclosure.

3 188. Northwell breached its fiduciary duty to Plaintiffs by failing to implement sufficient
4 safeguards and by disclosing Plaintiffs' and other Class Members' Private Information to
5 unauthorized third parties.
6

7 189. As a direct result of Northwell's breach of its fiduciary duty of confidentiality and
8 the disclosure of Plaintiffs' confidential Private Information, Plaintiffs and the Class Members have
9 suffered damages.

10 190. As a direct result of Northwell's breach of its fiduciary duty and the disclosure of
11 Plaintiffs' and Class Members' Private Information, Plaintiffs and the Class have suffered damages,
12 including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk
13 of identity theft, loss of privacy, confidentiality, embarrassment, emotional distress, and
14 humiliation.
15

16 191. Plaintiffs and the other Class Members suffered and will continue to suffer damages
17 including, but not limited to: (i) the untimely and/or inadequate notification of the Breach; (ii)
18 improper disclosure of the Private Information; (iii) loss of privacy; (iv) out-of-pocket expenses
19 incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by
20 the Breach; (v) the value of their time spent mitigating identity theft and/or identity fraud and/or the
21 increased risk of identity theft and/or identity fraud; (vi) the increased risk of identity theft; (vii) loss
22 of the benefit of the bargain; and (viii) emotional distress. At the very least, Plaintiffs and the Class
23 are entitled to nominal damages.
24

25 **COUNT IV**
26 **Unjust Enrichment**
27 **(On Behalf of Plaintiffs and the Class)**

28 192. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully
set forth herein.

1 193. This Count is pleaded in the alternative to all other claims and remedies at law.

2 194. Plaintiffs and Class Members conferred a benefit on Defendants by turning over their
3 valuable Private Information to Defendants in exchange for cybersecurity measures sufficient to
4 protect their Private Information from unauthorized access and disclosure. Plaintiffs and Class
5 Members did not receive such protection.
6

7 195. Upon information and belief, Defendants funds their data security measures entirely
8 from their general revenue, including from payments made to it by or on behalf of Plaintiffs and
9 Class Members.

10 196. As such, a portion of these payments made to Defendants are to be used to provide a
11 reasonable and adequate level of data security that is in compliance with applicable state and federal
12 regulations and industry standards, and the amount of the portion of each payment made that is
13 allocated to data security is known to Defendants.
14

15 197. Defendants has retained the benefits of their unlawful conduct, including the amounts
16 of payment received from or on behalf of Plaintiffs and Class Members, which payment should have
17 been used for adequate cybersecurity practices that it failed to provide.

18 198. Defendants knew that Plaintiffs and Class Members conferred a benefit upon it,
19 which Defendants accepted. Defendants profited from these transactions and used the Private
20 Information of Plaintiffs and Class Members for business purposes, while failing to use the payments
21 it received for adequate data security measures that would have secured Plaintiffs' and Class
22 Members' Private Information and prevented the Data Breach.
23

24 199. If Plaintiffs and Class Members had known that Defendants had not adequately
25 secured their Private Information, they would not have agreed to allow such Private Information to
26 be provided to Defendants.

27 200. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under
28 the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

201. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) an increase in spam calls, texts, and/or emails; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

202. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

203. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
Violations of the New York Deceptive Acts and Practices Act
N.Y. Gen. Bus. Law § 349 ("GBL")
(On Behalf of Plaintiffs and the Class Against Northwell)

204. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

205. Northwell violated New York’s General Business Law § 349(a) when it engaged in deceptive, unfair, and unlawful trade, acts, or practices in conducting trade or commerce and through furnishing of services, including but not limited to:

- a. Misrepresenting material facts to Plaintiffs and the Class by stating it would, *inter alia*, “make sure that information the identifies [Plaintiffs and Class Members] is kept private”;⁴⁴
- b. Misrepresenting material facts, including by representing itself as a business that would comply with state and federal laws pertaining to the privacy and security of Private Information belonging to Plaintiffs and the Class;
- c. Omitting and/or concealed material facts regarding its inadequate privacy and security protections for Private Information belonging to Plaintiffs and the Class;
- d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain sufficient privacy and security related to Private Information belonging to Plaintiffs and the Class resulting in a data breach, which is in violation of duties imposed on Defendant by state and federal laws, including the Federal Trade Commission Act (15 U.S.C. § 45);
- e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to Plaintiffs and the Class in a timely and accurate manner, which violates duties imposed on Defendant by New York General Business Law § 899-aa(2).

206. Northwell knew, or should have known, that its computer systems and security practices were inadequate to protect Private Information entrusted to Northwell by Plaintiffs and the

⁴⁴ <https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf>.

1 Class. Further, Northwell knew, or should have known, that the risk of theft of Private Information
2 through a data breach was highly probable, particularly given that cybercriminals have increasingly
3 targeted healthcare providers.

4 207. Northwell was in a superior position to know the true facts regarding its deficient
5 data security and should have disclosed this fact to the Plaintiffs and the Class.

6 208. Northwell mislead consumers regarding the security of its network and ability to
7 secure Private Information it collected by failing to disclose the true facts regarding its deficient data
8 security. This constitutes false and misleading representation, which had the capability, tendency,
9 and impact of deceiving or misleading consumers.

10 209. Northwell's representations were material representations, which consumers such as
11 Plaintiffs and the Class relied upon to their detriment.

12 210. The representations as well as Defendant's conduct towards Plaintiffs and the Class
13 occurred in New York where Plaintiffs and the Class engaged the services of and entrusted their
14 Private Information to Northwell.

15 211. Northwell's conduct is unconscionable, deceptive, and unfair, and is substantially
16 likely to and did mislead consumers such as Plaintiffs and the Class acting reasonably under the
17 circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class
18 have been injured because they were not timely notified of the Data Breach causing their Private
19 Information to be compromised.

20 212. As a direct and proximate result of Northwell's unconscionable, unfair, and deceptive
21 acts and omissions, Plaintiffs and the Class had their Private Information disclosed to unauthorized
22 third parties, which caused damage to Plaintiffs and the Class.

23 213. Plaintiffs and the Class seek relief under New York General Business Law § 349(h),
24 including actual damages or statutory damages of \$50 (whichever is greater), treble damages,
25 injunctive relief, and/or attorney's fees, expenses, and costs.
26
27
28

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

- a. An order certifying this action as a Class action;
- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 14, 2023

Respectfully submitted,

/s/ Nathan R. Ring

Nathan R. Ring

Nevada State Bar No. 12078

STRANCH, JENNINGS & GARVEY, LLC

2100 W. Charleston Boulevard, Suite 208

Las Vegas, NV 89102

A. Brooke Murphy (*pro hac vice* forthcoming)

MURPHY LAW FIRM

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Tel: (405) 389-4989
abm@murphylegalfirm.com

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY
PLLC

